ICT DIVISION
FUTURE IS HERE

BANGLADESH COMPUTER COUNCIL
COMPUTER FOR EVERYTHING

BGD e-GOV CIRT

TLP:CLEAR

Detection of Fog Ransomware Footprint in Cyber Space of Bangladesh

[This page is intentionally left blank]

TLP: CLEAR
Distribution: Public
Type of Threat: Ransomware

Date: 12 September 2024

Executive Summary

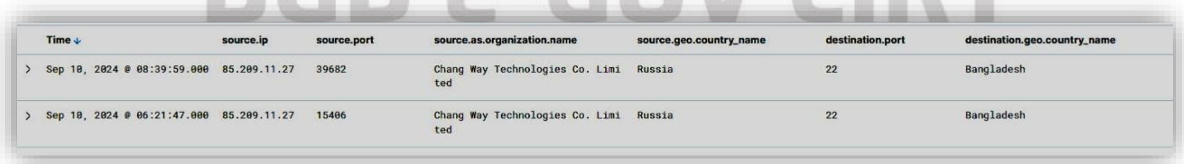
The Bangladesh e-Government Computer Incident Response Team (BGD e-GOV CIRT) has identified multiple IP addresses linked to the Fog Ransomware group (aka Lost in Fog) within Bangladesh. These addresses appear to originate from Russia, suggesting that the attackers might be operating from or routing their activities through that region. However, the exact location of the attackers remains uncertain due to their use of advanced masking techniques, such as proxy servers or VPNs, which obscure their true geographic location and complicate tracing efforts. Based on previous incidents involving the Fog Ransomware group, the attack may have been initiated after the attackers gained access through compromised VPN credentials. Once inside the networks, they could target both Windows and Linux systems, indicating a broad and potentially coordinated attack affecting a wide range of IT environments within Bangladesh.

Targeted Sectors:

- Educational Sector
- Banking and Non-Banking Financial Institutions
- Corresponding Service Providers to Financial Institutions
- Recreational sector

Fog Ransomware’s Footprint in Bangladesh:

Here we have found foot prints of IOC for FOG Ransomware in Bangladesh



	Time ↓	source.ip	source.port	source.as.organization.name	source.geo.country_name	destination.port	destination.geo.country_name
>	Sep 10, 2024 @ 08:39:59.000	85.209.11.27	39682	Chang Way Technologies Co. Limited	Russia	22	Bangladesh
>	Sep 10, 2024 @ 06:21:47.000	85.209.11.27	15406	Chang Way Technologies Co. Limited	Russia	22	Bangladesh

Fog ransomware at a glance:

Aspect	Details
Ransomware Family	STOP/DJVU
First Observed	2021
Primary Attack Vector	Exploits vulnerabilities in compromised VPN credentials to gain network access

Target Sectors	Primarily targets education and recreation sectors; recently observed targeting financial services and U.S. education networks (since May 2024).
Privilege Escalation Techniques	Uses advanced techniques like pass-the-hash attacks to escalate privileges to an administrative level, increasing its impact
Actions After Infiltration	- Disables protective security mechanisms - Encrypts critical files (especially Virtual Machine Disks) - Deletes backup data
File Encryption	Encrypted files are typically marked with extensions such as '.FOG' or '.FLOCKED'
Ransom Note	Accompanied by a ransom note that directs victims to a negotiation platform on the Tor network
Geographic Origin	Suspected to originate from Russia, though masking techniques (e.g., VPNs or proxies) make the true location uncertain
Attribution	No direct link to established APT groups, suggesting it may originate from a new, highly skilled threat actor
Recent Activity	Recently got its IOC's at several organizations of **Bangladesh**
Impact on Victims	Victims are left with little choice but to consider paying the ransom due to loss of backups and encryption of critical files
Communication Channel	`xql562evsy7njcsngacphcerzjfecwotdkobn3m4uxu2gtqh26newid[.]onion`

Attacker TTP (Tactic, Technique, Procedure):

Initial Access

- **T1133: External Remote Services**
  Attackers leveraged external remote services to gain initial access into the network.

- **T1078: Valid Accounts**
  Compromised VPN credentials were used by the attackers to gain access to the environment.

Discovery

- **T1046: Network Service Discovery**
  Attackers initiated network discovery by pinging endpoints and saving the results in text files.
  Tools: SoftPerfect Network Scanner (for Windows, macOS, and Linux), Advanced Port Scanner (free network and port scanner).
  Commands: `'pings.txt', 'pingw.txt', 'Advanced_Port_Scanner_2.5.3869(1).exe'`

Lateral Movement

- **T1135: Network Share Discovery**
  Attackers used SharpShares (an open-source tool for enumerating accessible network shares) to identify shared resources within the network.

- **T1021: Remote Services**
  Attackers exploited compromised service accounts to move laterally across systems and abuse domain trust relationships.
  Sub-techniques:
  - T1021.001: Remote Desktop Protocol
  - T1021.002: SMB/Windows Admin Shares

  Commands: `nltest /domain_trusts`, `'SharpShares.exe'`

- **T1570: Lateral Tool Transfer**
  Attackers used PsExec, a tool that allows remote execution of processes on other systems with full interactivity for console applications.

- **RDP and SMB Activity**
  Suspicious Remote Desktop Protocol (RDP) and Server Message Block (SMB) activity was observed, with files being encrypted via high-volume read/write operations.

- **Remote Access Tools**
  Attackers employed legitimate remote access tools, such as AnyDesk and SplashTop, for command-and-control (C2) communication.
  Tools: *AnyDesk (download[.]anydesk[.]com), SplashTop*

Credential Access

- **T1003: OS Credential Dumping**
  Attackers dumped credentials from the system, including encrypted Google Chrome credentials.
  Sub-techniques:
  - T1003.003: NTDS

  Commands:
  ```
  cmd.exe /Q /c esentutl.exe /y
  "C:\Users\USERNAME\AppData\Local\Google\Chrome\User Data\Default\Login
  Data" /d
  "C:\Users\USERNAME\AppData\Local\Google\Chrome\User Data\Default\Login
  Data.tmp"
  ```

- **T1555: Credentials from Password Stores**
  A PowerShell script (Veeam-Get-Creds.ps1) was used to obtain credentials from the Veeam Backup and Replication Credentials Manager.

- **T1110: Brute Force**
  Attackers attempted credential stuffing to compromise additional accounts.
  Sub-technique:
  - T1110.004: Credential Stuffing

- **Data Backup and Credential Theft**

  Attackers backed up login data from compromised endpoints, including encrypted credentials from Google Chrome.

  Commands:
  ```
  cmd.exe /Q /c esentutl.exe /y
  "C:\Users\USERNAME\AppData\Local\Google\Chrome\User Data\Default\Login
  Data" /d
  "C:\Users\USERNAME\AppData\Local\Google\Chrome\User Data\Default\Login
  Data.tmp"
  ```

Persistence

- **T1136: Create Account**

  Attackers created local administrator accounts to maintain persistence within compromised systems.

  Sub-technique:
  - T1136.001: Local Account (Administrator)

Execution

- **T1059: Command and Scripting Interpreter**

  Attackers used the Windows command shell to execute malicious commands.

  Sub-technique:
  - T1059.003: Windows Command Shell

- **T1569: System Services**

  Attackers used PsExec for service execution to run malicious processes on remote systems.

  Sub-technique:
  - T1569.002: Service Execution

Defense Evasion

- **T1562: Impair Defenses**

  Attackers disabled or modified tools such as Windows Defender and antivirus software to avoid detection.

  Sub-technique:
  - T1562.001: Disable or Modify Tools (Windows Defender/AV)

- **T1550: Use Alternate Authentication Material**

  Attackers used Pass the Hash to authenticate using captured hashes.

  Sub-technique:
  - T1550.002: Pass the Hash

- **T1078: Valid Accounts**

  Attackers continued to use compromised valid accounts for further malicious activities.

- **T1140: Deobfuscate/Decode Files or Information**
  Attackers deobfuscated and decoded information for further actions.

- **T1070: Indicator Removal**
  Attackers placed ransom notes and deleted system shadow copies to prevent file restoration.
  Sub-technique:
  - T1070.004: File Deletion

  Commands: `'readme.txt'`, *WMIC, PowerShell*

- **Data Transfer**
  Attackers used Rclone to sync and transfer data from compromised endpoints, focusing on recent files and excluding certain types.
  Tools: *Rclone*

- **Ransom Note and Data Destruction**
  Attackers placed ransom notes and deleted volume shadow copies to inhibit recovery.
  Commands: `'readme.txt'`, *WMIC, PowerShell*

Impact

- **T1486: Data Encrypted for Impact**
  Attackers spread ransomware to encrypt files and lock systems.
  Commands: `C:\programdata\locker.exe -id xCcNKl -nomutex -size 10 -console -target \HOSTS.DOMAIN.COM\SHAREDRIVE`

- **T1490: Inhibit System Recovery**
  Attackers used vssadmin.exe to delete volume shadow copies, preventing file restoration.

- **T1489: Service Stop**
  Attackers stopped services to increase the impact of the attack.

- **Ransom Note Details**
  The ransom note contained an introduction to the Fog ransomware group, detailing encryption and payment instructions.
  File: *'readme.txt'*

- **Double Extortion**
  Attackers threatened to publicly expose sensitive information if the ransom was not paid.

Indicators of Compromise (IOCs):

Type	Indicator	Description
SHA1	f7c8c60172f9ae4dab9f61c28ccae7084da90a06	Fog ransomware binary (lck.exe)
	507b26054319ff31f275ba44ddc9d2b5037bd295	Fog ransomware binary (locker_out.exe)
	e1fb7d15408988df39a80b8939972f7843f0e785	Fog ransomware binary (fs.exe)
	83f00af43df650fda2c5b4a04a7b31790a8ad4cf	Fog ransomware binary (locker_out.exe)
	44a76b9546427627a8d88a650c1bed3f1cc0278c	Fog ransomware binary (mon.dll)
	eeafa71946e81d8fe5ebf6be53e83a84dcca50ba	PsExec (psexesvc.exe)
	763499b37aacd317e7d2f512872f9ed719aacae1	Advanced Port Scanner (advanced_port_scanner.exe)
	3477a173e2c1005a81d042802ab0f22cc12a4d55	Advanced Port Scanner (advanced_port_scanner_2.5.3869.exe)
	90be89524b72f330e49017a11e7b8a257f975e9a	SharpShares (sharpshares(1).exe)
Filename	readme.txt	Ransom note
	DBgLog.sys	Log file created by ransomware binary
	Veeam-Get-Creds.ps1	PowerShell script used to obtain passwords from Veeam Backup and Replication Credentials Manager
	PSEXESVC.exe	PsExec
	netscan.exe	SoftPerfect Network Scanner
File Extension	.flocked	Appended file extension to encrypted files
	.fog	
IP Address	5.230.33[.]176	IP address used by the threat actor to login to VPN appliance
	77.247.126[.]200	
	107.161.50[.]26	
	85.209.11[.]227	
	85.209.[.]254	
	85.209.11[.]27	

Actions Required:

To mitigate the risk of potential cyber-attacks, BGD e-GOV CIRT recommends the following measures:

1. **Use Multi-Factor Authentication (MFA)**: Implement MFA for all VPN connections to mitigate the risk of compromised credentials.
2. **Regularly Update and Patch VPN Software**: Ensure all VPN applications are up to date with the latest security patches to address known vulnerabilities.
3. **Monitor VPN Access**: Employ monitoring tools to detect suspicious activities, such as unusual login attempts or access from unfamiliar locations.
4. **Isolate Affected Endpoints**: Implement automated isolation procedures that trigger when ransomware is detected to contain the threat.
5. **Utilize a Comprehensive Security Platform**: Use effective platforms to monitor network traffic/communications, logs, events etc. and respond to threats in real-time.
6. **Disable Unnecessary Services**: Avoid using Windows Management Instrumentation Command-line (WMIC) and PowerShell scripts unless absolutely necessary.
7. **Regularly Backup Critical Data**: Maintain up-to-date backups stored offline or in a secure, immutable environment to ensure data recovery.
8. **Apply the Principle of Least Privilege**: Restrict administrative privileges to minimize the potential impact of a successful attack.
9. **Conduct Regular Security Audits**: Regularly audit network and endpoint security to identify and address vulnerabilities.
10. **Establish Incident Response Plans**: Develop and test incident response plans to effectively detect, contain, and recover from ransomware attacks.
11. **Monitor Network Traffic**: Use advanced threat detection to monitor network traffic for signs of lateral movement or other suspicious activities.
12. **Cyber Security Awareness Training/ Session:** Necessary to conduct cybersecurity awareness training for all employees to educate them about potential cyber-attacks
13. **Report Incidents:** Report or inform BGD e-GOV CIRT regarding any cyber incident, IOC's, suspicious activities within your infrastructure, through mail id: cirt@cirt.gov.bd

Previous Alert and Guideline on Ransomware:

BGD e-GOV CIRT has previously published reports and advisories aiming at raising the awareness to combat such security incidents. You can find them in the following links:

1. Ransomware Prevention & First Response Guideline https://www.cirt.gov.bd/ransomware-prevention-first-response-guideline-english-version-1/
2. https://www.cirt.gov.bd/ransomware-service-providers-of-fin-institutions

References:

1. https://darktrace.com/blog/lifting-the-fog-darktraces-investigation-into-fog-ransomware
2. https://adlumin.com/post/fog-ransomware-now-targeting-the-financial-sector
3. https://arcticwolf.com/resources/blog/lost-in-the-fog-a-new-ransomware-threat